infoblox

Threat Intel

DNS-RÄUBER-ANGRIFF: VIPERS UND HAWKS KAPERN SITTING DUCKS-DOMAINS

Autoren:
Infoblox Threat Intel

INHALTSVERZEICHNIS

EINFÜHRUNG

Alles begann mit einer Lookalike-Domain. Die Domain war so gestaltet, dass sie wie eine Slack-Hosting-Ressource aussah, aber sie wurde in Russland gehostet. Einfaches Phishing? Vielleicht. Allerdings gab es auch eine merkwürdige Umleitungskette. Eine seit langem registrierte CBS Interactive-Domain wurde verwendet, um potenzielle Opfer auf ein gefälschtes Slack-Portal umzuleiten.[1] Könnte der Fernsehsender die Domain wirklich aufgegeben haben? Nein, sie war immer noch bei Mark Monitor registriert. Bei der Überprüfung des DNS-Auflösungsverlaufs wurde jedoch deutlich, dass die Domain, nachdem sie eine Zeit lang inaktiv war, in Russland aufgelöst wurde. Sie muss gekapert worden sein. Damals, im Januar 2024, ging man davon aus, dass die Entführung einer hochwertigen Domain wie `clickermediacorp[.]com` ein Zeichen für den Diebstahl von Zugangsdaten war. Wir meldeten das Hijacking sowohl dem Registrar als auch dem DNS-Anbieter und zogen weiter.

Ein paar Monate später kam das Thema des mysteriösen Domain-Hijackings wieder auf. Die Forscher von Proofpoint verfolgten ein kriminelles Traffic-Distributionssystem (TDS) namens 404TDS, das mit der Verbreitung von Malware und anderen bösartigen Inhalten in Verbindung stand. Unser Fachgebiet ist die Erkennung von DNS-Bedrohungen. Wo andere nach Malware suchen, die sie zurückentwickeln können, oder nach Webseiten, die sie analysieren können, erkennen wir die Fingerabdrücke der Akteure in der Art und Weise, wie sie DNS-Einträge konfigurieren und im Anschluss an ihre Aktivitäten eine Spur von Abfragen hinterlassen. Wir lieben TDS-Akteure, weil ein TDS von Natur aus mit DNS-Konfigurationen verwoben ist und wir oft in der Lage sind, Muster zu erkennen, die es uns ermöglichen, das TDS zu überwachen, während es sich entwickelt, anstatt auf bösartige Nutzdaten zu warten. Wir gingen davon aus, dass es eine DNS-Signatur für 404TDS geben muss.

Als wir begannen, nach einem Mechanismus zu suchen, um die 404TDS zu verfolgen, wurde schnell klar, dass alle Domains gekapert worden waren, einschließlich `clickermediacorp[.]com`. Aber die Bandbreite dieser Hijackings war ungewöhnlich groß, und die Erklärung des Diebstahls von Zugangsdaten oder des Hacks von Registrierstellen ergab keinen Sinn.

1 https://urlscan.io/result/8ee644c6-2ad3-4cd9-a0e6-e05ad01ade5d/

Wir haben uns mit einem Eclypsium-Forscher zusammengetan und versucht, eine Erklärung für das weit verbreitete Domain-Hijacking im Zusammenhang mit 404TDS zu finden.

Wir entdeckten, dass falsch konfigurierte DNS-Nameserver der gemeinsame Faktor bei allen Hijackings waren und dass wir falsch konfigurierte Domains bei bestimmten Providern mit ein paar Tastenklicks übernehmen konnten. Obwohl wir Experten für DNS-Bedrohungen sind, war dies neu für uns. Und nicht nur für uns – vor der Veröffentlichung im Juli 2024 sprachen wir mit einer Vielzahl von Personen in der Regierung und der Industrie, in der Bedrohungsforschung und in Netzwerken. Niemand, mit dem wir in den ersten Monaten gesprochen haben, war sich des Angriffsvektors bewusst und schon gar nicht seiner massenhaften Ausnutzung. Brian Krebs erinnerte sich daran, dass er über eine große Kampagne berichtet hatte, bei der diese Technik zum Einsatz kam. Zum Zeitpunkt seiner Berichterstattung sah es jedoch so aus, als handele es sich um ein Problem bei einem einzelnen Registrar und nicht um ein systemisches Problem.[2] Schließlich stießen wir auf den ursprünglichen Bericht von Matt Bryant über die Schwachstelle, die wir als Sitting Ducks bezeichnet hatten, und stellten fest, dass die Angreifer den Angriffsvektor wahrscheinlich schon seit mindestens acht Jahren unentdeckt genutzt hatten.[3]

Unser erstes Paper über Sitting Ducks sollte das Bewusstsein für eine wenig bekannte Hijacking-Technik schärfen und konkrete Maßnahmen für Domaininhaber und Registranten zur Sicherung ihrer Domains aufzeigen. Wir hofften, dass dies nicht nur Kriminelle zum Handeln anregen würde. In unserer Nachforschung haben wir festgestellt, dass diese anfälligen Bereiche oft das Ergebnis von Fusionen, Übernahmen und der durch personelle Veränderungen verlorenen Datenverläufe sind. Während die Domain `clickermediacorp[.]com` nach unserem Juli-Bericht gesichert wurde, bleiben leider andere CBS-Domains anfällig. *Wenn Sie dies lesen und Hilfe benötigen, rufen Sie uns an.* Wir arbeiteten mit einer Opferorganisation zusammen, um ihre Domains zu reparieren, weil sie das Wissen über die Domains, aber auch über die Anmeldeinformationen des Registrars verloren hatten. Und im alarmierendsten Fall haben wir mit Besitzern von .gov zusammengearbeitet, um ihre Konfigurationen zu korrigieren.

Seit unserer ersten Veröffentlichung haben wir fast 800.000 gefährdete registrierte Domains identifiziert. Etwa neun Prozent (70.000) dieser anfälligen Domains wurden anschließend gekapert. Wir wissen, dass diese Zahlen die Angriffsfläche nicht genau widerspiegeln: Sie stammen von einem begrenzten Überwachungssystem. Die Herausforderung bei einem Sitting Ducks-Angriff besteht darin, dass er leicht durchzuführen und sehr schwer zu entdecken ist. Cyberkriminelle haben diesen Vektor seit mindestens 2018 verwendet, um über 80.000 Domänennamen zu kapern, darunter auch solche im Besitz bekannter Marken, gemeinnütziger Organisationen und staatlicher Stellen.

Sitting Ducks ist nicht der einzige konfigurationsorientierte Angriffsvektor, den wir in diesem Jahr gesehen haben: Es wurden auch mehrere Arten von CNAME-Hijackings und sogar eine WHOIS-Server-Übernahme gemeldet.[4,5] Auch Regierungen und Normungsgremien spielen eine wichtige Rolle beim Schutz der Nutzer vor dieser Art von Angriffen. Nationale und multinationale Organisationen sollten das Bewusstsein für die Risiken aller konfigurationsbezogenen Probleme schärfen und Anreize zur Risikominderung schaffen. Dazu gehören auch Sicherheitsanforderungen, die Schutzmaßnahmen gegen Angriffe wie DNS-Hijacking beinhalten. Leider konzentrieren sich viele Regierungsorganisationen, darunter auch die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA), auf Software-Schwachstellen. Daher erfüllen Konfigurationsschwachstellen ungeachtet ihrer potenziellen kriminellen Auswirkungen nicht die Voraussetzungen für die Einstufung als CVE. Beispielsweise ist selbst für Registranten einer .gov TLD lediglich die Nutzung eines „kompetenten“ DNS-Providers erforderlich. Wir haben festgestellt, dass die Folge davon ist, dass bestimmte Registrierstellen eine lahme Delegation für neue Domänenregistrierungen erstellen, indem sie die Konfiguration einer Nameserver-Einstellung erzwingen, bevor die DNS-Providereinträge erstellt werden. Es ist ein Wettlauf mit der Zeit, den wir aber immer wieder beobachten können. Die fehlende Aufmerksamkeit für diese

2 https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

3 https://thehackerblog.com/floating-domains-take-over-20k-digitalocean-domains-via-a-lax-domain-import-system/

4 https://labs.guard.io/subdomailing-thousands-of-hijacked-major-brand-subdomains-found-bombarding-users-with-millions-a5e5fb892935

5 https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/

Art von Problemen lässt ihre Ausbeutung weitgehend unvermindert weiterlaufen. Es bleibt zu hoffen, dass sowohl Schulungen zur Sensibilisierung als auch proaktive Maßnahmen entwickelt werden, die nicht nur den Angriffsvektor der Sitting Ducks, sondern die gesamte Klasse der Konfigurationsschwachstellen abdecken.

Eine allzu häufige Reaktion ist es, mit dem Finger auf den Domaininhaber zu zeigen, der letztlich die Verantwortung für die Pflege seiner Domainkonfigurationen trägt. Das mag stimmen, aber gleichzeitig können sowohl Registrierstellen als auch DNS-Anbieter eine entscheidende Rolle bei der Eindämmung der Cyberkriminalität spielen, indem sie diese Art von Hijacks erschweren oder leichter beheben. Während unserer Recherchen meldeten wir Sitting Ducks-Hijackings sowohl bei Registrierstellen als auch bei DNS-Anbietern, aber es wurde weitgehend abgetan und nicht gehandelt, obwohl wir Beweise für die Angriffe lieferten. In vielen Fällen waren wir nicht in der Lage, die Domaininhaber zu informieren, weil sie private Registrierungsdaten verwendet hatten. In mehreren Fällen, in denen wir mit kompromittierten Domaininhabern zu tun hatten, wussten diese nicht, dass sie die Domains besaßen, da der Speicher und die Dokumentation im Laufe der Zeit und durch Unternehmensfusionen verloren gegangen waren. Die Unfähigkeit, Domäneninhaber zu erreichen, bedeutet, dass sowohl Registrare als auch DNS-Anbieter realistisch gesehen eine aktivere Rolle bei der Reaktion auf Informationen von Threat Intelligence-Organisationen spielen und den Missbrauch ihrer Plattformen und Benutzer minimieren sollten, um die Kriminalität zu reduzieren.

Bei der Untersuchung des Angriffsvektors entdeckten wir mehr als ein Dutzend unabhängiger Akteure, die ihn ausnutzen. In diesem Beitrag erläutern wir einige davon, darunter den Betreiber von 404TDS und VexTrio Viper. Wir stellen auch zwei neue Akteure vor, die wir verfolgen: Horrid Hawk und Hasty Hawk.

Das Ziel dieses Artikels ist es, zu zeigen, auf welche Weise diese gekaperten Domains verwendet werden, damit sie leichter identifiziert und deaktiviert werden können. Wir werden Folgendes teilen:

- Wie man einen Sitting Ducks-Angriff vermeiden und eine kompromittierte Domain identifizieren kann
- Wie verschiedene Bedrohungsakteure Sitting Ducks-Angriffe nutzen, um eine Infrastruktur zu schaffen, die gegen die Erkennung durch Sicherheitsanbieter resistent ist
- Wie sich einige Sitting Ducks-Bedrohungsakteure miteinander verbinden, was auf eine Art Informationsaustausch oder Schattenwirtschaft für gekaperte Domains hindeutet
- Wie einige Domains, die mit großen Marken verbunden sind, wiederholt gekapert werden, oft von verschiedenen Bedrohungsakteuren
- Und wie wichtig DNS für die Erkennung und Verfolgung dieser hartnäckigen Bedrohungsakteure ist.

DER ANGRIFFSVEKTOR „SITTING DUCKS“

Beginnen wir zunächst mit einer Zusammenfassung. Im Juli haben wir gemeinsam mit Eclypsium einen Bericht zu einem weit verbreiteten und wenig beachteten Angriffsvektor veröffentlicht, den wir „Sitting Ducks“ nennen.[6] Bei diesem Angriff erlangt der böswillige Akteur die vollständige Kontrolle über die Domain, indem er die DNS-Konfigurationen kontrolliert. Sie können die Domain auch kapern, ohne Anmeldedaten zu stehlen oder sich Zugang zum Konto des Domaininhabers zu verschaffen – sehr raffiniert. In den meisten Fällen wurden diese Domains oder Subdomains von ihrem ursprünglichen Besitzer vergessen, sodass der Angriff unbemerkt bleibt. Wir haben mehr als ein Dutzend Bedrohungsakteure beobachtet, die diese gekaperten Domains für eine Vielzahl von kriminellen Aktivitäten wie die Verbreitung von Malware, Command and Control (C2), Phishing, Traffic Distribution System (TDS)-Operationen und mehr missbrauchen.

Ein Sitting Ducks-Angriff nutzt Fehlkonfigurationen in den DNS-Einstellungen für eine Domain aus, insbesondere wenn das DNS auf den falschen autoritativen Nameserver zeigt. Es gibt einige Bedingungen, die erfüllt sein müssen, damit ein Angreifer eine Domain auf diese Weise kapern kann: Eine registrierte Domain oder die Subdomain einer registrierten Domain nutzt

6 https://blogs.infoblox.com/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

oder delegiert autoritative DNS-Dienste an einen anderen Anbieter als den Domain-Registrar; dies wird **Delegierung genannt**.

- Die Delegierung ist **„lahm“**, was bedeutet, dass die autorisierenden Nameserver des Eintrags keine Informationen über die Domäne haben und daher Abfragen nicht lösen können.
- Der maßgebliche DNS-Provider ist **ausnutzbar**, d. h. der Angreifer kann die Domain beim Provider „beanspruchen“ und DNS-Einträge einrichten, ohne Zugriff auf das Konto des gültigen Besitzers bei der Domainregistrierungsstelle zu haben.

Abbildung 1 zeigt eine übliche Sitting Ducks-Angriffssequenz. Es gibt mehrere Varianten dieser Art von Angriff, von denen keine die Kompromittierung der legitimen DNS-Infrastruktur erfordert, wodurch sie sich grundlegend von bekannteren DNS-Hijacking-Techniken unterscheidet. Zu den Varianten dieses Angriffs gehören die erneute Delegierung an einen anderen DNS-Anbieter und die teilweise lahme Delegierung, was bedeutet, dass nur einige der autoritativen Nameserver falsch konfiguriert sind. Die niedrige technische Zugangsbarriere gibt vielen verschiedenen Cyberkriminellen Gruppen die Möglichkeit, die Sicherheitslücke auszunutzen. Das führt zu mehr Angriffen, die aufgrund des positiven Rufs, den viele dieser gekaperten Domains haben, schwer zu erkennen sind.

Sitting Ducks-Angriffe sind zwar leicht durchzuführen und schwer zu erkennen, aber mit den richtigen Konfigurationen bei der Domainregistrierungsstelle und den DNS-Providern sind sie durchaus vermeidbar. Nicht alle DNS-Anbieter sind jedoch ausnutzbar. Nachdem wir etwa ein Dutzend davon ausgewertet haben, haben wir bestätigt, dass täglich Hunderte von Domain-Hijackings bei ausnutzbaren Providern stattfinden: Wir haben seit August etwa 800.000 registrierte Domains mit lahmen Delegationen identifiziert, aber die tatsächliche Zahl ist viel höher; wir haben anfällige Subdomains nicht berücksichtigt und unsere Suche auf bestimmte Provider beschränkt.

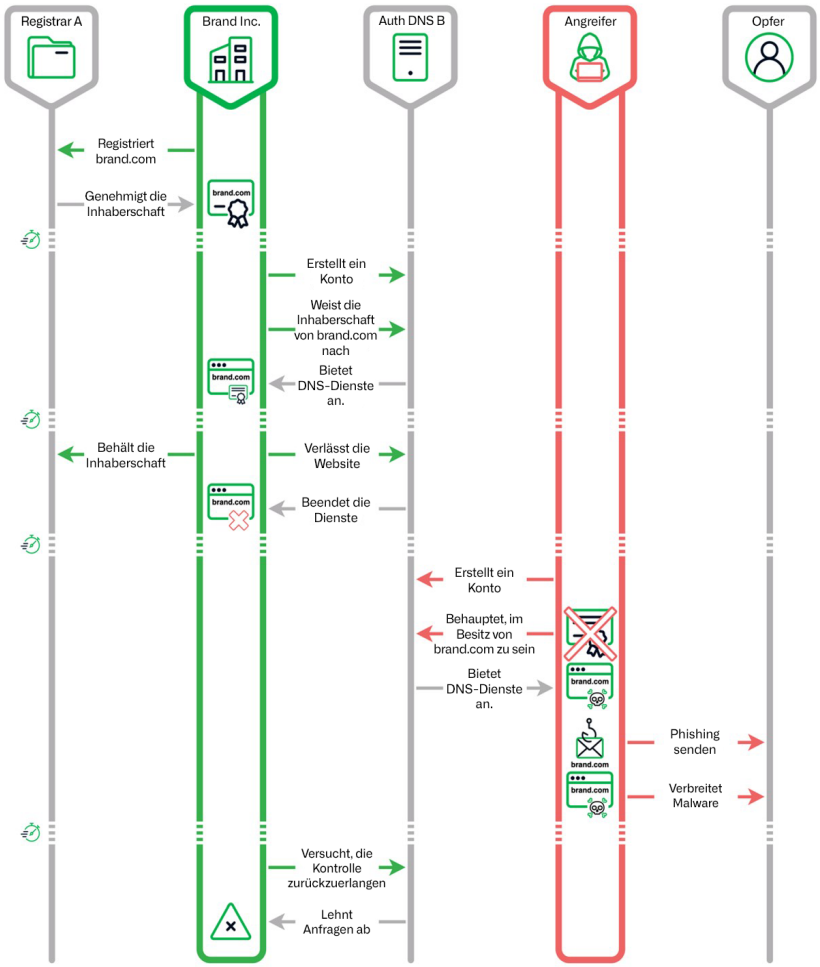

Abbildung 1. Eine typische Sitting Ducks-Angriffssequenz

Es ist noch nicht bekannt, wie Bedrohungsakteure anfällige Domains bei verschiedenen Anbietern identifizieren. Wir haben mehrere Erkennungsmethoden eingesetzt und dabei festgestellt, dass zwischen sechs und zehn Prozent der Domains, die an einem bestimmten Tag ausnutzbaren DNS-Anbietern zugewiesen wurden, lahm sind. Bei einigen ausnutzbaren Providern war die Zahl der angreifbaren Domains deutlich höher. Da unsere Tests begrenzt waren, ist die wahre ausnutzbare Landschaft wahrscheinlich viel größer, als wir heute wissen. Insgesamt schätzen wir, dass über 1 Million registrierte Domains an einem bestimmten Tag für einen Sitting Ducks-Angriff anfällig sind. Die meisten gefährdeten Domänen, die wir entdeckt haben, haben Nameserver, die einem der wenigen DNS-Anbieter zugewiesen sind.

Sehen wir uns nun einige der Akteure an, die diesen Angriffsvektor verwenden.

VACANT VIPER

Was verbirgt sich hinter einem Namen?

Vacant Viper ist der Name, den wir dem Bedrohungsakteur gegeben haben, der das 404TDS betreibt, das zuerst von Proofpoint gemeldet wurde.[7] Infoblox benennt etablierte Akteure oder Infrastrukturkomponenten grundsätzlich nicht um. Wenn wir von 404TDS sprechen, meinen wir den TDS selbst, und wenn wir von Vacant Viper sprechen, meinen wir den Akteur, der Domains für 404TDS kapert und andere bösartige Aktivitäten wie Spam durchführt.

Während wir 404TDS für eine DNS-Signatur untersuchten, die vorhersagen könnte, dass eine Domain Teil der TDS-Infrastruktur werden würde, stellten wir fest, dass die Domains gekapert wurden. Bei genauer Betrachtung der kompromittierten Domains schien es außerdem, dass der Akteur mehr vorhatte als nur ein kriminelles TDS zu betreiben. Wir nannten den Entführer „Vacant Viper“, wobei wir unsere Viper-Kategorie als Anspielung auf die TDS-Ursprünge verwendeten.

Vacant Viper ist einer der ersten bekannten Bedrohungsakteure, die Sitting Ducks ausnutzen, und hat seit Dezember 2019 jedes Jahr schätzungsweise 2.500 Domains gekapert. Dieser Akteur nutzt die gekaperten Domains, um bösartige Spam-Aktionen durchzuführen, Pornos zu versenden, RAT (Remote Access Trojan) C2s einzurichten und Malware wie DarkGate und AsyncRAT zusammen mit ihren 404TDS-Aktionen zu verbreiten.[8] Zu den gemeldeten Tochtergesellschaften gehören TA-866 und TA-571.

Vacant Viper missbraucht die DNS-Unternehmen von DigiCert, bevorzugt aber kostenlose Konten bei DNS Made Easy, die für eine 30-tägige Testphase verfügbar sind und für deren Einrichtung nur eine E-Mail-Adresse erforderlich ist. Sie haben jedoch auch Domains bei Constellix gekapert, einem Premium-DNS-Dienst, der vor einer kostenlosen Testphase die Kontaktaufnahme mit Vertriebsmitarbeitern erfordert. Seit wir im Juli 2024 zum ersten Mal über die Angriffe der Sitting Ducks berichtet haben, hat der Akteur seine Techniken angepasst, operiert aber weiterhin ausschließlich mit dieser Gruppe von Anbietern. Der Umfang des Hijackings variiert im Laufe der Zeit, aber wir haben zum Beispiel in den ersten beiden Wochen des Oktobers 2024 etwa 100 Domains identifiziert, die von Vacant Viper gekapert wurden.

Vacant Viper kapert keine Domains für eine bestimmte Markenverbindung, sondern für eine Reihe von Ressourcen, die einen guten Ruf haben und von Sicherheitsanbietern nicht blockiert werden. Vacant Viper entführt auch einige Domains wiederholt im Laufe der Zeit. Zum Beispiel wurde `clickermediacorp[.]com` im Januar 2024 als Teil des 404TDS gesehen und mit einer Phishing-Kampagne in Verbindung gebracht, die Slack imitierte, aber die Domain wurde zuvor im Januar 2020 verwendet, um eine Vielzahl von Inhalten zu liefern, darunter Pornografie und Bitcoin-Betrug.

Ein wesentliches Merkmal eines TDS ist, dass es Partner gibt: Anbieter, die Datenverkehr in das TDS senden, und Kunden, die Datenverkehr vom TDS erhalten. In der Welt der Werbung besteht das Ziel eines TDS darin, den Gewinn zu maximieren, d. h. die Nutzer zu der Anzeige zu leiten, die ihnen am ehesten gefällt. Das Ziel eines kriminellen TDS ist ähnlich: Benutzer mit Inhalten zu ködern, die sie höchstwahrscheinlich konsumieren möchten, und sie dann zu den

7 https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

8 https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

bösartigen Inhalten zu leiten, sei es ein Malware-Download, eine gefälschte Anmeldeseite oder ein Geschenkkartenbetrug.

Die folgenden Beispiele von 404TDS-Angriffsketten zeigen Umleitungstechniken, die sowohl von den TDS als auch von ihren Partnern verwendet werden, einschließlich der Art und Weise, wie Vacant Viper gekaperte Domains in den 404TDS verwendet.

Eine Domain, die Vacant Viper gekapert und in den 404TDS verwendet hat, ist `mcpennsylvania[.]com`, eine Domain, die von McDonald's bei CSC Corporate Domains registriert und Nameservern auf DNS Made Easy, einer Tochtergesellschaft von DigiCert, zugewiesen wurde.[9] Vacant Viper hat diese Domain in den letzten Jahren wiederholt gekapert, und sie hat zum jetzigen Zeitpunkt eine lahme Delegation. Zuletzt haben wir beobachtet, dass diese McDonald's-Domain auf `ncbtv[.]com` (ehemals von einem IPTV-Dienstanbieter betrieben) umgeleitet wird, die 2011 bei GoDaddy registriert wurde, ursprünglich mit einer chinesischen E-Mail-Adresse. Ironischerweise scheint auch diese Domain, die jetzt unter privater Registrierung steht, mehrfach von einem Sitting-Ducks-Angriff gekapert worden zu sein, möglicherweise schon 2017. Zuletzt wurde `ncbtv[.]com` mit VexTrio Viper in Verbindung gebracht, einem Bedrohungsakteur, der gekaperte Domains verwendet, um Dating-Sites und andere Inhalte zu hosten. Unter der Annahme, dass dieser Akteur unabhängig von Vacant Viper ist, können wir sehen, dass Bedrohungsakteure, die Sitting Ducks-Angriffe verwenden, miteinander kooperieren und wahrscheinlich Wissen und/oder Ressourcen für anfällige Domänen teilen.

Im Juni 2023, als Vacant Viper `mcpennsylvania[.]com` kaperte, nutzten sie es für 404TDS in einer AsyncRAT-Malware-Angriffskette und nutzten zwei verschiedene Mechanismen (Meta-Refresh und HTTP-Refresh), um den Benutzer umzuleiten:[10]

- Die URL `hXXps://mcpennsylvania[.]com/y0t/gojhuovy` zeigte einen 404-Fehler (Not Found), aber im Hintergrund wurde ein Meta-Refresh durchgeführt, um den Benutzer über den HTML-Meta-Tag umzuleiten:
  - `<meta http-equiv=”refresh” content=”0;hXXps://ecole-artcom[.]com/wdown”>`
- Die zweite URL `hXXps://ecole-artcom[.]com/wdown/` antwortete ohne Inhalt außer einem aktualisierten HTTP-Header, der den Benutzer effektiv erneut auf eine dritte URL umleitete
- Die dritte URL `hXXps://www[.]mediasimulasi[.]com/wazxd` hinterließ eine JavaScript-Datei namens Information_28_jun_1220107.js, die anschließend mit AsyncRAT verknüpfte Dateien herunterlud.[11]

Es ist nicht bekannt, wer die Landing Domains kontrolliert, sie wurden bisher nur in Verbindung mit 404TDS beobachtet. Wir zeigen die Header für die `mcpennsylvania[.]com`-Angriffskette in Abbildung 2.

9 https://who.is/whois/mcpennsylvania.com

10 https://urlscan.io/result/14797fe3-beaf-4949-9d04-6edcf94b25aa/#transactions

11 https://github.com/executemalware/Malware-IOCs/blob/main/2023-07-05%20AsyncRAT%20IOCs

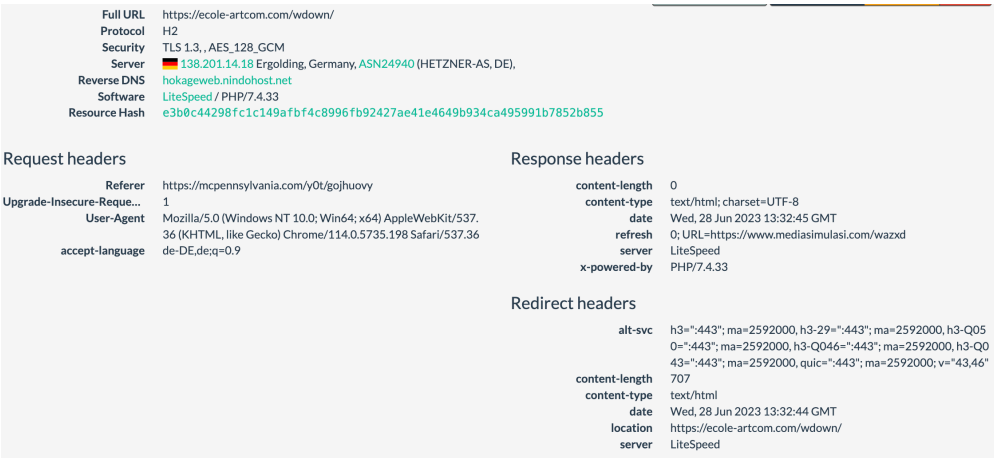

Abbildung 2. Aktualisierungsheader leiteten Benutzer zu `hXXps://www[.]mediasimulasi[.]com/wazxd`

Vacant Viper verwendete auch die HTML-Meta-Refresh-Technik in Angriffsketten, die DarkGate-Malware über bösartige Spam-Anhänge verbreiteten. Die Umleitungskette für die Verbreitung der DarkGate-Malware[12] ähnelt AsyncRAT, enthält aber nicht die Hypertext Transfer Protocol-Aktualisierungsmethode:

1. Der Benutzer versucht, `afarm[.]net` zu erreichen, was zu einem 404 Not Found-Fehler führt
2. Die TDS-URL `hXXps://afarm[.]net/uvz2q` leitet dann über die `HTML-Meta-Refresh-Methode` <meta http-equiv=”refresh” content=”0;hXXps://wercosliuhqgheirn[.]com/”> zu `https://wercosliuhqgheirn[.]com/ weiter`.
3. Der Benutzer wird zu `hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php` weitergeleitet, wo die folgende Datei mit der DarkGate-Malware heruntergeladen wird:

Dateiname	SHA-256-Hash
08-May-24-document-53aa77b6.jar	f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a

Die acht Domains in Tabelle 1 folgen alle dem gleichen Umleitungsmuster, um die gleiche JAR-Datei zu liefern, die mit DarkGate verbunden ist.[13] Wir haben sechs dieser Domänen in ähnlich benannten Spam-Dateianhängen gesehen, z. B. may-document_85138492.pdf, im Mai 2024. All diese Dateien werden als Anhänge bösartiger Spam-E-Mails mit einer ähnlichen allgemeinen Nachricht verbreitet, in der auf eine angehängte Rechnung oder ein Spesendokument verwiesen wird, das der Benutzer öffnen soll, damit er die Zahlung vornehmen kann.

`aerospaceavenue[.]com`
`affixio[.]com`
`adventsales[.]co[.]uk`
`afarm[.]net`
	`affiliatebash[.]com`
	`amikamobile[.]com`
	`afcmanager[.]net`
	`adztrk[.]com`

Tabelle 1. Entführte Domains, die Vacant Viper zur Verbreitung der DarkGate-Malware verwendet hat

12 https://urlscan.io/result/1f4d4a62-8a6f-4452-b64c-1d38b3cd6086/#summary

13 https://bazaar.abuse.ch/sample/f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a#intel

Die Nachforschungen von Vacant Viper führten nicht nur zur (Wieder-)Entdeckung des Sitting Ducks-Angriffsvektors, sondern ermöglichten es uns auch, andere Bedrohungsakteure mit diesem Angriffsvektor in Verbindung zu bringen. Einige dieser Akteure wurden aufgespürt, andere nicht. Im Allgemeinen haben wir festgestellt, dass es äußerst schwierig ist, eine kompromittierte Domain selbst zu entdecken. Wir haben das Verhalten der Bedrohungsakteure genutzt, um eine Signatur zu erstellen, die dann verfolgt werden kann. Für Bedrohungsakteure, die DNS-Hijacking nutzen, verwenden wir die Benennungskategorie eines Hawk.

Warum ein Hawk?

Diese Bedrohungsakteure stürzen sich auf anfällige Domains, ähnlich wie Falken, die im Sturzflug nach ihrer Beute greifen.

HORRID HAWK

Horrid Hawk ist ein DNS-Bedrohungsakteur, der seit mindestens Februar 2023 Domains kapert und sie für Anlagebetrugsprogramme verwendet. Sie sind interessant, weil sie bei jedem Schritt ihrer jüngsten Kampagnen gekaperte Domains verwenden und überzeugende Köder über nicht existierende staatliche Investitionsprogramme oder Gipfeltreffen auslegen. Sie betten die gekaperten Domains in kurzlebige Facebook-Anzeigen ein, die sich an Nutzer in über 30 Sprachen auf mehreren Kontinenten richten. Wir verfolgen Horrid Hawk über DNS und haben fast 5.000 ihrer gekaperten Domains identifiziert.

Eine Horrid Hawk-Angriffskette umfasst zwei verschiedene gekaperte Domains. Meistens wurden sie von einigen wenigen DNS-Anbietern gekapert: Linode, TierraNet und A2 Hosting. Nachdem sie eine Domain gekapert haben, konfiguriert Horrid Hawk die IP-Adresse des A-Eintrags auf einen anderen dedizierten Server um. Der Akteur weist eine der Domains einem TDS-Server zu, der die Landingpage vor Sicherheitsforschern abschirmt und unerwünschte Webbesucher herausfiltert. Horrid Hawk weist die andere Domäne der Landing Page zu, die betrügerische Investitionsinhalte beherbergt. Schon früh in ihrer Geschichte registrierte Horrid Hawk auch eigene ähnliche Domains, die zu den Themen der staatlichen Investitionen passen, wie `oil-poland[.]site` und `balticpipe[.]playroom8[.]site`. Der Akteur nutzte diese Domains für seine Landingpages, die Inhalte im Zusammenhang mit Gasprojektbetrug enthielten. Abbildung 3 zeigt die Zeitleiste von zwei Domains, die sie gekapert und zusammen in einem Angriff verwendet haben.

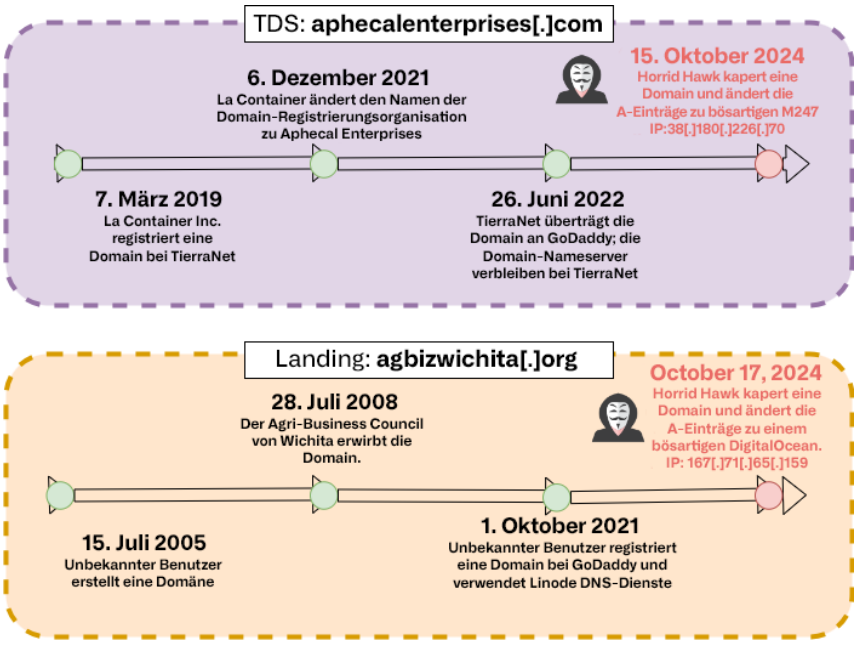

Abbildung 3. Zeitleiste der Domain-Hijackings von `aphecalenterprises[.]com` *(TDS) und* `agbizwichita[.]org` *(Landingpage-Domain)*

Horrid Hawk macht Jagd auf Verbraucher auf der ganzen Welt. Sie beginnen ihre Angriffe mit der Erstellung vieler Facebook-Anzeigen wie der in Abbildung 4, die sich an Benutzer in Polen richtet und für ein gefälschtes, staatlich finanziertes Gasprojekt, die Baltic Pipe, wirbt. Das in der Facebook-Anzeige verwendete Bild enthält eine Nachricht, die Benutzer über 50 auffordert, auf den Anzeigenlink zu klicken und den Inhalt des Webartikels zu lesen. Diese Facebook-Werbekampagne erreichte über 13.000 Internetnutzer. Obwohl es sich bei dem Beispiel, das wir in diesem Abschnitt verwenden, um eine Kampagne handelt, die sich an ältere polnischsprachige Benutzer richtet, verwendet Horrid Hawk auch Phishing-Köder auf Englisch, Italienisch, Türkisch, Spanisch und in vielen anderen Sprachen.

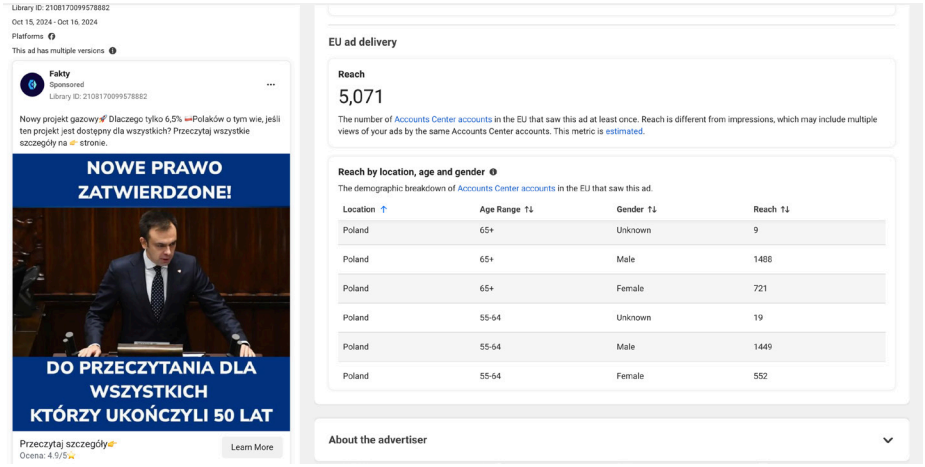

Abbildung 4. Beispiel einer Facebook-Werbung von Horrid Hawk, die sich an polnischsprachige Nutzer richtet, die meist über 55 Jahre alt sind

Der in Abbildung 4 gezeigte Werbelink zeigt auf hXXps://aphecalenterprises[.]com/, eine URL, die vom Horrid Hawk TDS-Server verwendet wird. Dieses System ist für den Bedrohungsakteur wichtig, da es die Landingpage des Betrugs schützt, indem es ein Profil der Webbesucher erstellt und irrelevante und unerwünschte Gäste, wie Sicherheitsforscher und Web-Scraping-Bots, herausfiltert. Der Server verwendet geografische Informationen, um den nächsten URL-Standort des Webbesuchers zu bestimmen. Wenn ein Benutzer beispielsweise von einer in Polen ansässigen IP-Adresse zu hXXps://aphecalenterprises[.]com/ navigiert, leitet Horrid Hawk ihn auf die Betrugs-Webseite der Regierung um, die sich unter hXXps://agbizwichita[.]org/9fMS3XSS befindet. Der zufällige URL-Pfad 9fMS3XS ist nur vorübergehend, und diese Webseite lädt eine statische Datei (/lander/long-ready-2_0/index.html), auf die das Basis-HTML-Attribut href verweist. Abbildung 5 ist die Webseite, die wir sahen, als diese URL noch aktiv war.

Abbildung 5. Politisch motivierte Betrugs-Webseite (hXXps://agbizwichita[.]org/lander/long-ready-2_0/index.html), die sich an polnischsprachige Benutzer richtet

Befindet sich die IP-Adresse des Website-Besuchers in einem Land, das für die Zielgruppe von Horrid Hawk irrelevant ist, werden diese Benutzer in der Regel auf eine gefälschte Webseite umgeleitet, die dieselbe TDS-Domäne verwendet. Als wir zum Beispiel `aphecalenterprises[.]com` mit einer IP-Adresse außerhalb Polens besuchten, zeigte uns der TDS eine harmlose Webseite an, die ein Online-Kleidungsgeschäft imitierte. Abbildung 6 zeigt die URL-Struktur und den Inhalt der Täuschungswebseite. URLs für Lockvogel-Webseiten enthalten einen Dateinamen mit dem statischen Präfix `w-{Ländercode}-`. Der Ländercode war in diesem Fall „pl“, eine Abkürzung für das Zielland Polen, und das „w“ steht möglicherweise für „White Cover“ oder „White Label“.

Abbildung 6. Eine Köderwebseite, die von Horrid Hawk TDS für nicht zielgerichtete Webbesucher bereitgestellt wird

Das am weitesten verbreitete Thema, das wir auf den verschiedenen Webseiten gesehen haben, bezieht sich auf das „Baltic Pipe Project“, ein Investitionsprogramm, das behauptet, dass polnische Bürger, die in neue Gaspipelines investieren, große Geldsummen verdienen können. Im obigen Beispiel handelt es sich dabei um die `agbizwichita[.]org`-Landingpage. Horrid Hawk verwendet eine Panikmache, die sich die natürliche Angst der Menschen, etwas zu verpassen (FOMO), zunutze macht. Auf der Webseite wird behauptet, dass Bürger, die sich nicht an dem staatlich finanzierten Gasprojekt beteiligen, einen Anstieg der gasbezogenen Ausgaben um 55 % erleiden werden. Ähnlich wie bei den Investitionskampagnen, die von einem anderen Akteur des Investitionsprogramms durchgeführt werden, über den wir in diesem Jahr berichtet haben, Savvy Seahorse,[14] forderte die Baltic Pipe-Kampagnen den Nutzer auf, seine persönlichen Daten, einschließlich Name, E-Mail und Telefonnummer, in ein eingebettetes Formular einzugeben, um sich für die Investitionsmöglichkeit zu registrieren. Die Benutzer werden dann darüber informiert, dass sie für weitere Informationen kontaktiert werden, bevor sie auf die „Investmentplattform“ zugreifen können. Abbildung 7. Obwohl andere Bedrohungsakteure Baltic Pipe-Betrügereien betreiben, zeichnet sich Horrid Hawk durch die Verwendung von Sitting Ducks-Angriffen aus, um Domains zu kapern.[15]

14 https://blogs.infoblox.com/threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/

15 https://urlscan.io/result/61541987-122b-484d-acdc-290f02f98a8b/

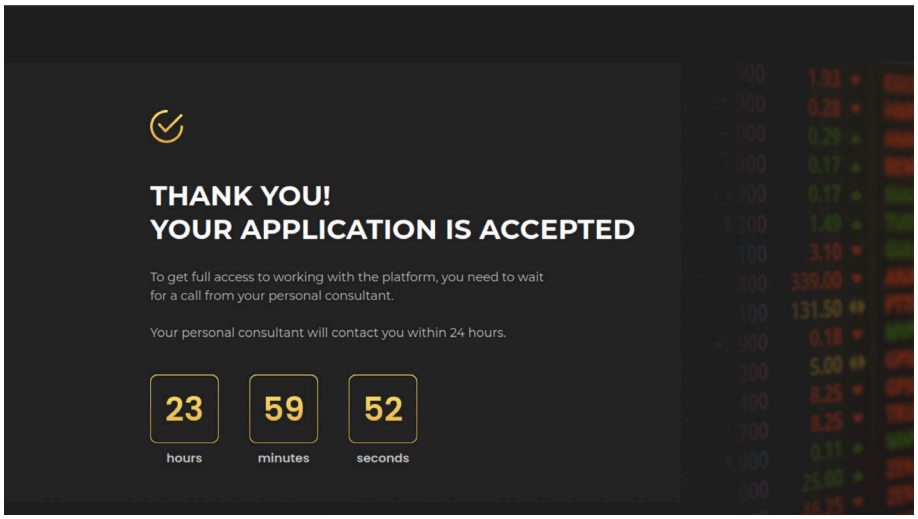

Abbildung 7. Eine typische Horrid Hawk-Antwortseite, die angezeigt wird, nachdem sich ein Opfer erfolgreich auf den Betrugs-Websites registriert hat

HASTY HAWK

Hasty Hawk ist ein weiterer Bedrohungsakteur, den wir bei unseren Recherchen zu Sitting Ducks-Entführungen entdeckt haben. Seit mindestens März 2022 hat Hasty Hawk über 200 Domains gekapert, um weit verbreitete Phishing-Kampagnen durchzuführen, die in erster Linie DHL-Versandseiten und gefälschte Spendenseiten fälschen, um die Ukraine zu unterstützen. Der Akteur nutzt viele Anbieter aus, darunter HawkHost, Maria Hosting und DigitalOcean. Die gekaperten Domains werden oft über DNS umkonfiguriert, um Inhalte auf russischen ASNs wie PROTON66 oder BEGET zu hosten, aber es ist auch bekannt, dass der Akteur andere Anbieter wie OVH verwendet. Hasty Hawk verwendet Google-Anzeigen und möglicherweise andere Mittel wie Spam-Nachrichten, um schädliche Inhalte zu verbreiten.

Die vollqualifizierten Domainnamen (FQDNs) von Hasty Hawk folgen in der Regel einigen Mustern wie den folgenden:

- `dhl.<random numbers>.<hijacked domain>`
- `dhl-id<random numbers>.<hijacked domain>`
- `<random numbers/letters>.dhl.<hijacked domain>`

Abbildung 8 zeigt die DNS-Eintragsänderungen für `thebagshelf[.]com` ab dem Erstellungsdatum und dem Tag, an dem es von Hasty Hawk gekapert wurde. Ähnlich wie Horrid Hawk konfiguriert auch Hasty Hawk die A-Eintragsadresse auf einen Server um, der dem Akteur gewidmet ist. Zusätzlich zu den DHL-Subdomain-Namenspräfixen wie `dhl[.]3204[.]thebagshelf[.]com` haben wir andere statische Subdomain-Namenspräfixe auf diesen Servern beobachtet, darunter `id-f<random number>.<hijacked domain>` (z. B.`id-f0596[.]successbusinesspages[.]com`).

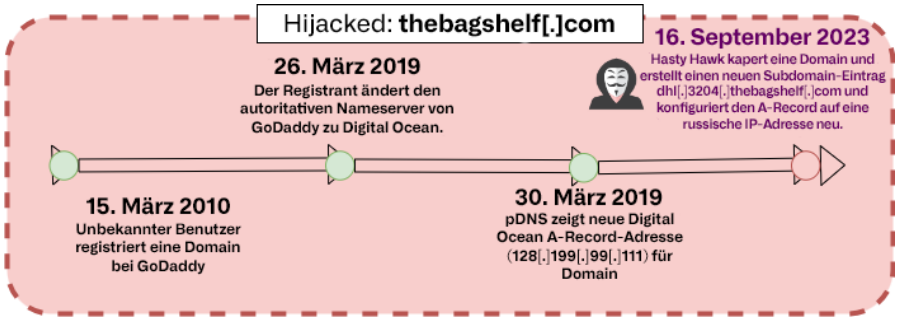

Abbildung 8. Zeitplan für Domain-Hijacking für `thebagshelf[.]com`

Hasty Hawk hat kürzlich viele seiner DHL-Webseiten in gefälschte Spendenseiten umgewandelt, die Spiegelkopien der legitimen Website `supportukrainenow[.]org` sind, die von der Organisation Global Shapers betrieben wird[16] um die Ukraine während des Krieges zu unterstützen (siehe Abbildung 9). Der Akteur hat auch Seiten erstellt, die die Europäische Union mit einer anderen gefälschten Spendenseite vortäuschen, die sich an Europäer richtet, die die Opfer des Krieges unterstützen wollen.

Abbildung 9. Gefälschte Spendenseite, die `supportukrainenow[.]org fälscht`

Hasty Hawk verwendet ein TDS, um Benutzer auf verschiedene Webseiten umzuleiten, deren Inhalt und Sprache sich je nach ihrem Standort und möglicherweise anderen Benutzereigenschaften unterscheiden. Wenn Benutzer je nach verwendetem Gerät, Standort oder zu unterschiedlichen Zeiten unterschiedliche Inhalte sehen, ist dies ein klares Anzeichen dafür, dass im Hintergrund ein TDS arbeitet, das sicherstellt, dass die Opfer auf die Seite umgeleitet werden, die den Kriminellen den größten Nutzen bringt. Hasty Hawk wechselt auch einige seiner Domains zwischen verschiedenen Kampagnenthemen hin und her. Sehen wir uns das Beispiel in Abbildung 10 an, mit geolokalisierungsbasierten Umleitungen und Änderungen des Webseiteninhalts im Laufe der Zeit für den FQDN `dhl[.]3204[.]thebagshelf[.]com`.

16 https://www.globalshapers.org/home

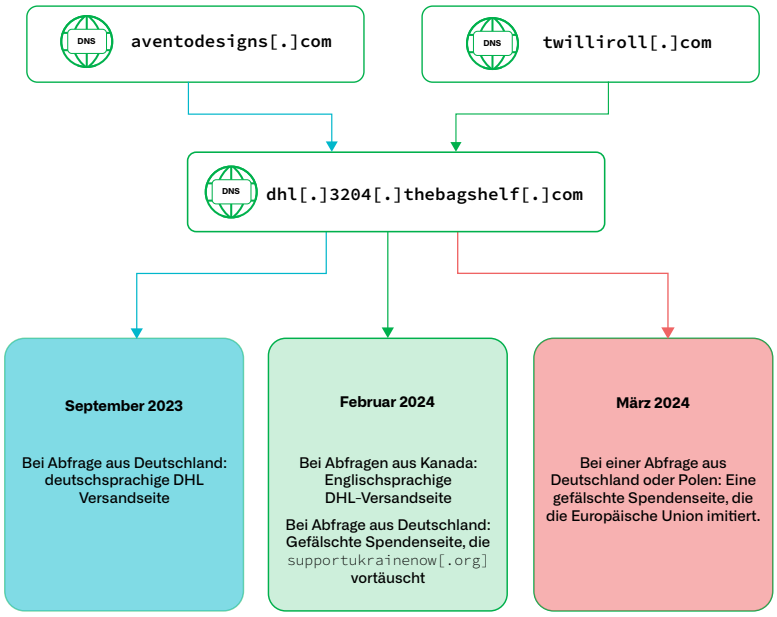

Abbildung 10: Beispiel für Umleitungen zu `dhl[.]3204[.]thebagshelf[.]com` *und einige der Webseiten, die der Akteur im Laufe der Zeit angezeigt hat*

1. **September 2023** – Der FQDN hostet eine deutschsprachige DHL-Versandseite. Die Benutzer wurden von `aventodesigns[.]com dorthin umgeleitet`.[17]
2. **Februar 2024** – Der FQDN hostet sowohl eine englischsprachige DHL-Versandseite (umgeleitet von `twilliroll[.]com`) für Benutzer in Kanada als auch die gefälschte Spendenseite, die `supportukrainenow[.]org` für Benutzer in Deutschland vortäuscht.
3. **März 2024** – Der FQDN wechselt die IPs von `91[.]212[.]166[.]71` zu `91[.]212[.]166[.]14` und hostet die Ukraine-Supportseite, die für Benutzer in Deutschland und Polen die Europäische Union vortäuscht.

Hasty Hawk änderte die Kampagnenthemen für diesen einzelnen FQDN im Laufe des Jahres 2024 weiter. Ab September hostete der FQDN die in Abbildung 11 gezeigte englischsprachige DHL-Versandseite oder leitete auf eine CAPTCHA-Seite weiter, die den Benutzer aufforderte, „die Sicherheitsüberprüfung abzuschließen, um auf `dhl[.]com` zuzugreifen“, und leitete als Köder auf die legitime DHL-Website weiter.[18]

17 https://urlscan.io/result/520f01c1-c3cf-48ad-9295-95bbd671ea50

18 https://urlscan.io/result/1998c142-5292-4895-98bd-17c04394286b

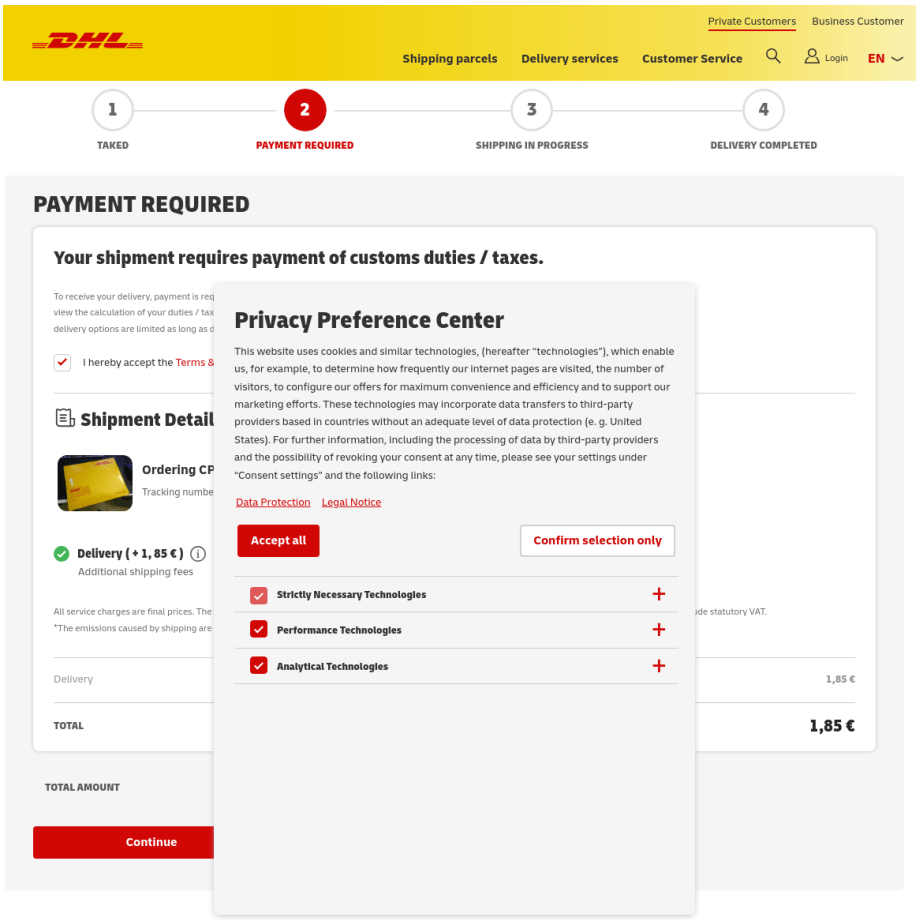

Abbildung 11. DHL-Phishing-Seite für `dhl[.]3204[.]thebagshelf[.]com` *im September 2024*

VEXTRIO VIPER UND PARTNER

Als wir bei unseren Nachforschungen immer mehr von Sitting Ducks gekaperte Domains entdeckten, erkannten wir, dass einige seit Anfang 2020 Teil der massiven VexTrio Viper TDS-Infrastruktur sind. Diese Domains fielen uns zunächst aufgrund ihres Alters auf, aber als wir entdeckten, dass sie gekapert worden waren, fügte sich das fehlende Teil an seinen Platz. Im Wesentlichen verwendet VexTrio Viper gekaperte Domains in seinem TDS auf ähnliche Weise wie Vacant Viper. VexTrio betreibt das größte cyberkriminelle Affiliate-Programm, das kompromittierten Web-Traffic von über 65 Affiliate-Partnern weiterleitet, von denen einige auch Domains über Sitting Ducks für ihre eigenen bösartigen Aktivitäten gestohlen haben.

VexTrio hat lahme Domains gekapert, die einst an DigiCert/DNS Made Easy (DME), Constellix und DigitalOcean-Nameserver delegiert wurden, um ihre TDS-Server zu betreiben. Die entführten Domänen leiten den Datenverkehr an die nachgelagerten Herausgeber bösartiger Inhalte oder an ihre eigenen bösartigen Websites weiter, auf denen gefälschte Dating- und Geschenkkartenbetrügereien, gefälschte CAPTCHA-Benachrichtigungen von Robotern usw. gehostet werden.

Eines der bemerkenswertesten Beispiele ist `mpinc[.]com`. Wir haben bestätigt, dass VexTrio die Domain im August 2023 gekapert hat, aber sie könnten sie bereits im April 2022 kompromittiert haben. Der ursprüngliche Eigentümer dieser Domain ist MPR Associates, eine Organisation, die sich auf Bildungsforschung konzentriert. Diese Domain war hauptsächlich in den 1990er und 2000er Jahren aktiv, bevor sie 2013 von RTI International (`rti[.]org`), einem gemeinnützigen Forschungsinstitut, das sich auf soziale, wissenschaftliche und gesundheitliche Fragen spezialisiert hat, übernommen wurde. Ende 2015 wurde die Domain auf DME-Nameserver umgestellt. Laut pDNS wurde `mpinc[.]com` an einem DigitalOcean IP

(157[.]230[.]67[.]179) ab Januar 2022 drei Monate lang „geparkt“, bevor es im April 2022 von einem Bedrohungsakteur, höchstwahrscheinlich VexTrio, gekapert wurde. Während die Domain von August bis Oktober 2023 unter der Kontrolle von VexTrio stand, leitete sie die Nutzer auf eine der in Abbildung 12 gezeigten häufig genutzten gefälschten Dating-Sites des Akteurs um.[19, 20] Derzeit befindet sich mpinc[.]com im „lahmen“ Zustand und wurde nicht an einen autoritativen DNS-Server delegiert.

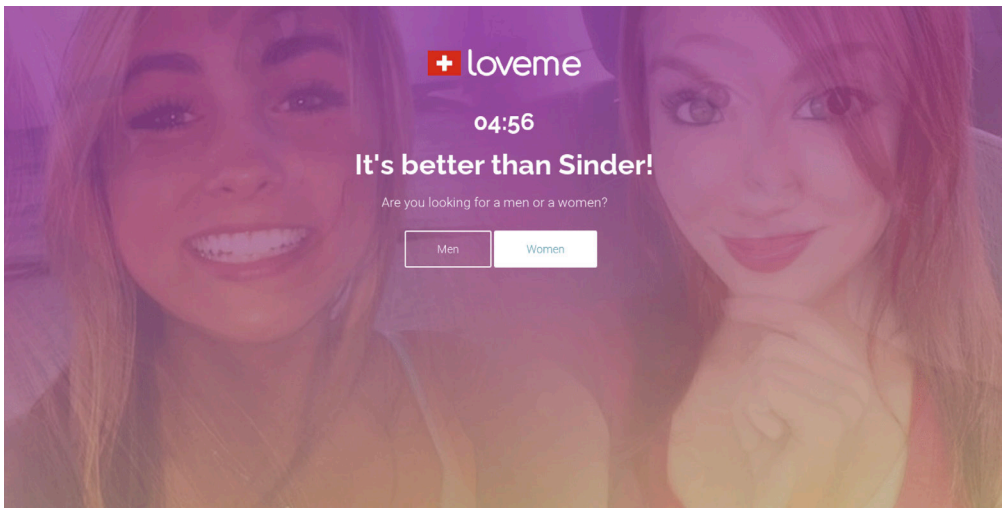

Abbildung 12. Gefälschte Dating-Webseite für die gekaperte Domain mpinc[.]com

VexTrio hat auch iccps[.]org gekapert, eine Domain, die zuvor für die jährliche ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) verwendet wurde. Die Domain wurde bereits im September 2009 von einem Professor der Carnegie Mellon University registriert. Nach den WHOIS-Informationen gehen wir davon aus, dass diese Domain, nachdem sie an DME-Nameserver delegiert wurde, ab Anfang August 2023 ausgenutzt werden konnte. VexTrio nutzte sie dann in seiner TDS-Infrastruktur und leitete Benutzer von September bis Oktober 2023 zu seinen Kampagnen weiter. Sie wurde dann auf die IP-Adresse von DigitalOcean aufgelöst, die für abgelaufene Domains verwendet wird, und wurde schließlich auf einer Bodis-IP geparkt, wo sie derzeit verbleibt. ACM/IEEE verwendet jetzt iccps[.]acm[.]org[21] für ihre Konferenz.

VEXTRIO VIPER-PARTNER VERWENDEN ANTIBOT CLOUD

Wir haben auch gesehen, dass VexTrio Viper-Partner Sitting Ducks ausnutzen. Viele von ihnen nutzen AntiBot Cloud, einen russischen Anti-Bot-Dienst, als Methode, um Bots und den Datenverkehr von Sicherheitsforschern herauszufiltern. Die Funktionalität von AntiBot umfasst die Möglichkeit, Regeln zum Blockieren bestimmter Bot-Dienste oder Benutzer auf der Grundlage ihrer Informationen, wie z. B. ihrer IP-Geolocation und ihres Nutzer-Agenten, festzulegen. Sie können diesen Dienst kostenlos lokal mit eingeschränktem Bot-Schutz nutzen oder auf die Cloud-Premium-Version upgraden. Oberflächlich betrachtet scheint AntiBot Cloud nicht von Natur aus bösartig zu sein, aber die Mehrheit der Benutzer scheint aus Cyberkriminellen zu bestehen. Der von russischen und anderen osteuropäischen Cyberkriminellen bevorzugte Dienst war ursprünglich auf Russisch verfasst, wurde später um englische Inhalte erweitert und bietet den russischen Rubel als eine seiner primären Zahlungsoptionen an (siehe Abbildung 13). AntiBot scheint vollständig von einer Person mit dem Pseudonym MikFoxi verwaltet zu werden, die sich selbst als freiberuflicher Programmierer bezeichnet. Es ist auch wichtig zu beachten, dass nur die Affiliates und nicht VextRIO Viper selbst AntiBot verwenden – das Blockieren von AntiBot blockiert VextRIO nicht. Die FQDNs für den AntiBot-Clouddienst umfassen:

19 https://urlscan.io/result/7948b668-5226-4670-9b54-63d1da91fee2

20 https://iccps.acm.org/2025/

21 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

- hXXps://antibotcloudapi[.]com/9.php
- antibotcloudapi[.]com
- antibot[.]cloud
- antibotcloud[.]com
- ipv4[.]mikifox[.]com
- ipv6[.]mikifox[.]com
- admin[.]mikifox[.]com

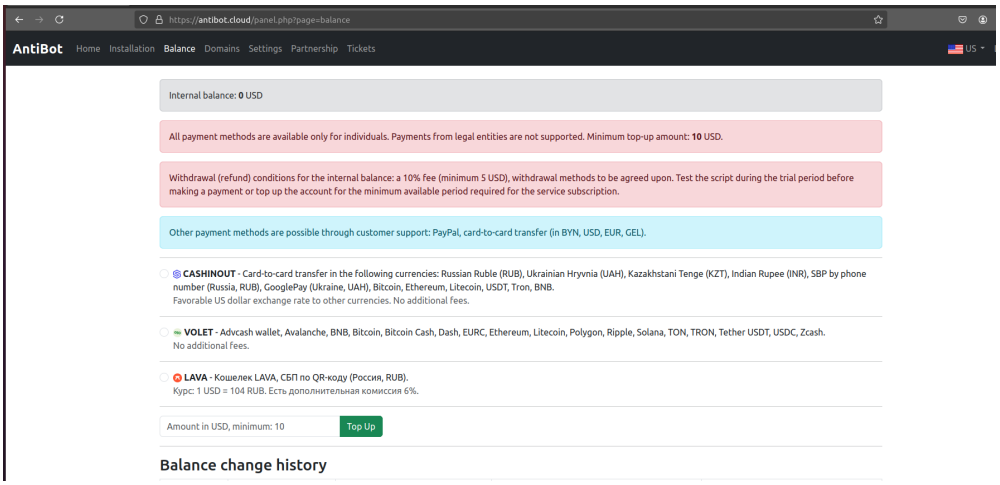

Abbildung 13. AntiBot-Zahlungsoptionen, einschließlich des russischen Rubels

Ein Partner, der AntiBot verwendet, hat missouri[.]com gekapert[22] per DME im Oktober 2022, aber diese Domain wurde möglicherweise schon früher von anderen Bedrohungsakteuren gestohlen. Während die Domain von diesem Partner kontrolliert wurde, wurden Benutzer auf eine gefälschte Dating-Site umgeleitet, die von VexTrio Viper betrieben wurde. Vor dem ersten Hijacking wurde die Website, die missouri[.]com nutzte, von State Ventures, LLC entwickelt und stand möglicherweise in Verbindung mit dem Bundesstaat Missouri. Die Domain zeigte zuvor eine große Anzahl von Subdomain-Einträgen, die den Städten und Landkreisen in Missouri gewidmet waren. Die zwischengespeicherten Daten zeigen, dass es sich um eine Website handelte, die reich an Inhalten war, die sich auf die Unternehmen und den Tourismus des Staates beziehen, wie in Abbildung 14 unten dargestellt. Darüber hinaus wurde die ehemalige Website der Missouri Lottery möglicherweise der Subdomain lottery[.]missouri[.]com zugewiesen. Ihr Inhalt wird jetzt bei molottery[.]com gehostet, das auch DME-Nameserver verwendet.

22 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

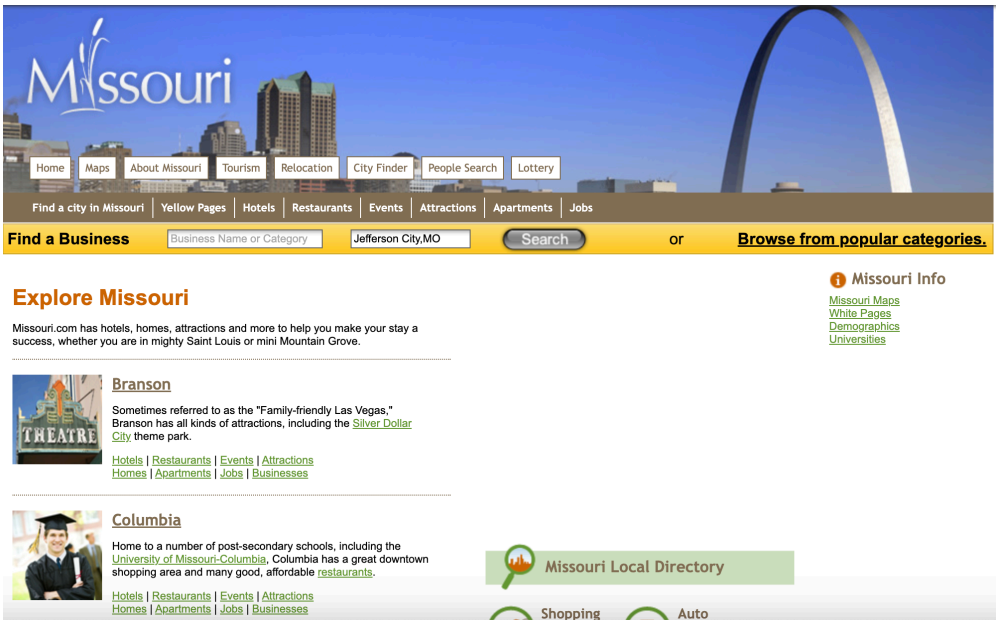

Abbildung 14. Webseite für `missouri[.]com` *im September 2018, möglicherweise die offizielle Seite des Bundesstaates Missouri, bevor sie gekapert wurde*

VEXTRIO GOREFRESH-PARTNER

GoRefresh ist ein Tochterunternehmen von VextRio Viper, das gefälschte Online-Pharmakampagnen durchführt und an Kampagnen anderer Partner wie Online-Glücksspiel oder Dating-Betrug teilnimmt. GoRefresh hat Domains der anfälligen DNS-Dienstanbieter DME und GoDaddy gekapert. Dieser Partner verwendet diese gekaperten Domains, um kompromittierten Web-Traffic zu VexTrio und anderen verbundenen Unternehmen sowie zu seinen eigenen Pharma-Landingpages umzuleiten.

Ähnlich wie Vacant Viper reagiert GoRefresh in der Regel mit einem „HTTP 404 Not Found“-Fehlerstatuscode auf Benutzer. Wenn sie alternativ eine Ressource als Redirector bereitstellen, verzichten sie auf die traditionelle HTTP-302-Weiterleitungsantwort und „aktualisieren“ stattdessen die Webseite des Opfers über eine HTML-Meta-Aktualisierung auf die nächste URL. Ein Beispiel für diese HTML-Codeumleitung:

```
<meta http-equiv=”refresh” content=”0;http://vipshopevent[.]su”>
```

ROTIERENDES HIJACKING

Ein häufiges Vorkommnis, das wir bei unseren Recherchen zu Sitting Ducks beobachtet haben, ist rotierendes Hijacking: wenn eine Domain im Laufe der Zeit von mehreren Akteuren gekapert wird. Bedrohungsakteure nutzen oft ausnutzbare Service Provider, die kostenlose Konten wie DNS Made Easy anbieten, als Leihbibliotheken und kapern Domains in der Regel für 30 bis 60 Tage; wir haben jedoch auch andere Fälle gesehen, in denen Akteure die Domain für einen langen Zeitraum halten. Nachdem das kurzfristige, kostenlose Konto abgelaufen ist, geht die Domain dem ersten Bedrohungsakteur „verloren“ und wird dann entweder geparkt oder von einem anderen Bedrohungsakteur beansprucht.

Wir haben gesehen, dass VexTrio Viper-Partner dies recht häufig tun, insbesondere wenn sie Domains entführen, die zuvor von Vacant Viper kompromittiert wurden. Als Beispiel zeigen wir in Abbildung 15 unten die Hijacking-Timeline für `mcpennsylvania[.]com`, die zunächst von Vacant Viper und später von einem VexTrio Viper-Partner gekapert wurde. Den WHOIS-Informationen zufolge blieben der Registrar (CSC Digital Brand Services) und der Nameserver-Anbieter (DME) während der verschiedenen Hijackings weitgehend unverändert.

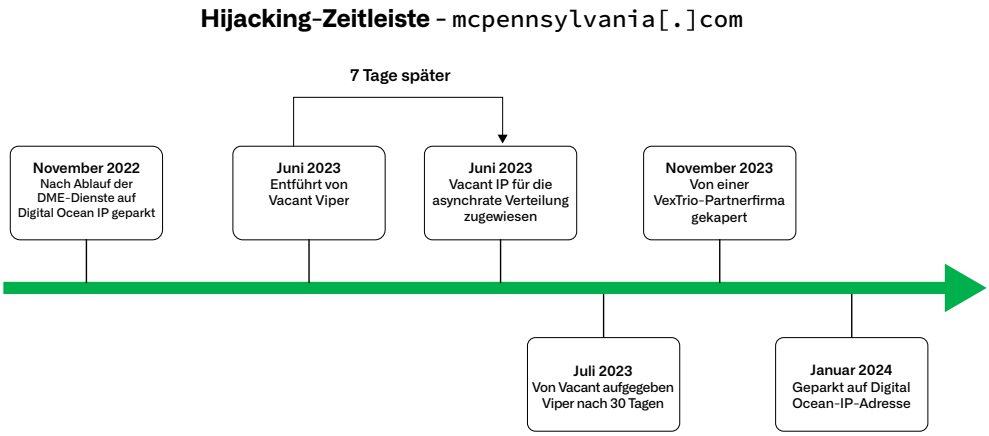

Abbildung 15. Zeitleiste der Entführung von mcpennsylvania[.]com

ZUSAMMENFASSUNG

Die von uns vorgestellten Bedrohungsakteure sind nur eine Auswahl derer, die aus diesem mächtigen und undurchsichtigen Angriffsvektor Kapital geschlagen haben. Die Auswirkungen des Angriffsvektors „Sitting Ducks“ sind zwar weitreichend, aber auch völlig vermeidbar, wenn auch kompliziert zu bekämpfen. Die Akteure werden diesen Angriffsvektor weiterhin ausnutzen, wenn keine aktiven Anstrengungen zur Eindämmung und letztlich zur Prävention unternommen werden. Wie wir in unserem Enthüllungs-Blog mitgeteilt haben, spielt jeder eine Rolle beim Stoppen von Sitting Ducks-Angriffen – von maßgeblichen DNS-Anbietern und Registrierstellen bis hin zu Regierungsorganisationen und Standardisierungsgremien. Wir brauchen bessere Möglichkeiten, um Hijackings zu erkennen und ihnen möglichst schnell Einhalt zu gebieten. Legitime Domain-Registranten müssen nicht nur ihre DNS-Einträge verwalten, sondern auch auf Missbrauchsberichte reagieren, ebenso wie Registrare und Anbieter.

Da dieser Angriff so schwer zu erkennen ist, besteht wenig Zweifel daran, dass Bedrohungsakteure ihn weiterhin nutzen werden. Wir haben mehrere Akteure ausfindig gemacht, die Domains gekapert und für längere Zeit gehalten haben, aber wir konnten den Zweck des Hijackings nicht feststellen. Diese Domänen genießen in der Regel ein hohes Ansehen und werden von Sicherheitsanbietern in der Regel nicht bemerkt. Dies schafft eine Umgebung, in der clevere Akteure ohne Konsequenzen Malware verbreiten, zügellosen Betrug begehen und Benutzeranmeldedaten fälschen können. Es bleibt zu hoffen, dass die Threat Intelligence-Community, sobald sie mehr über diese Technik weiß, den Einsatz der Akteure aufdecken und die Verfolgung und Remediation der gekaperten Domains ermöglichen.

Obwohl die Produkte von Infoblox nicht anfällig für „Sitting Ducks“ sind, können unsere Kunden dennoch betroffen sein, je nachdem, welche DNS-Betriebsart sie für die von ihnen registrierten Domänen gewählt haben. Daher empfehlen wir allen Inhabern von Domänennamen, insbesondere denjenigen, die DNS-Systeme von Drittanbietern verwenden und sich über deren Servicestatus nicht im Klaren sind, ihr Risikoniveau anhand der drei Fragen in Abbildung 16 zu bewerten.

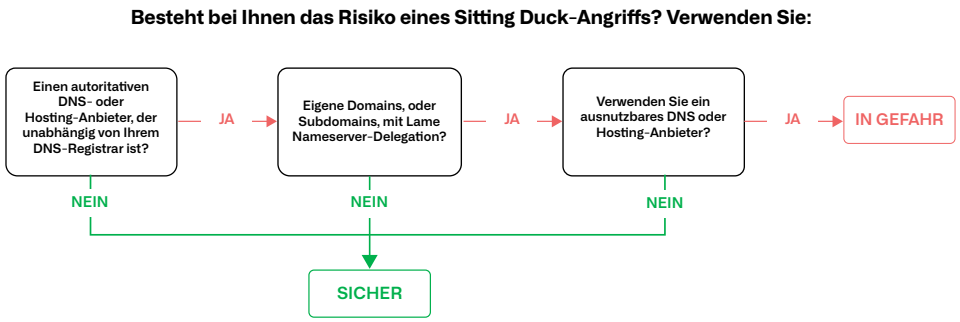

Abbildung 16. Drei Fragen, um festzustellen, ob Sie einem „Sitting Ducks“-Angriff ausgesetzt sind

OPFER VON SITTING DUCKS

Die gekaperten Domains, die wir in diesem Bericht beschreiben, gehörten legitimen Organisationen aus verschiedenen Branchen. Eine Domain kann während ihrer Lebensdauer mehrere verschiedene Eigentümer haben. Die folgende Liste enthält die rechtmäßigen Eigentümer, die wir vor dem Hijacking ihrer Domains identifiziert haben.

Gekaperte Domain	Rechtmäßiger Inhaber der Domain
agbizwichita[.]org	Agri-Business Council von Wichita
alonbyacarian[.]com	Acarian Systems Alon Capri Lautsprecher
aphecalenterprises[.]com	Aphecal Enterprises Inc.
clickermediacorp[.]com	CBS Interactive
iccps[.]org	Internationale Konferenz über Cyber-Physical Systems
jmnet[.]com	J.M. Eagle
mbhs[.]com	MISSISSIPPI BAPTIST HEALTH SYSTEMS, INC.
mcpennsylvania[.]com	McDonald's Corporation
missouri[.]com	State Ventures, LLC und möglicherweise der Staat Missouri
mosaicmedicalsupply[.]com	Mosaic Medical Supplies (orthopädischer und kosmetischer Lieferant)
mpinc[.]com	MPR Associates (Rechtsanwaltskanzlei)
mstouchenaturals[.]com	MS TOUCHE
mygemcon[.]com	Gemcon-Gruppe
ncbtv[.]com	NCBTV (IPTV-Dienstanbieter)
successbusinesspages[.]com	Success Business Pages (Online-Branchenbuch)
thebagshelf[.]com	Thailändisches Online-Bekleidungsgeschäft
tmsec[.]com	T&M USA (Privates Sicherheits- und Ermittlungsunternehmen)
uni-t[.]com	Bridgestone - Firestone Tire Sales Company

AKTIVITÄTSINDIKATOREN

Die nachstehende Tabelle enthält Indikatoren für die von diesen Bedrohungsakteuren verwendeten Aktivitäten (IOAs). Weitere Informationen finden Sie im Infoblox Threat Intelligence GitHub Repo: `https://github.com/infobloxopen/threat-intelligence/tree/main`.

Indikator	Typ	Anmerkung
`oil-poland[.]site` `balticpipe[.]playroom8[.]site`	Domain	Von Horrid Hawk registrierte und in ihren Kampagnen verwendete Lookalike-Domains

`mstouchenaturals[.]com`
`covidianmuseum[.]com`
`alhej[.]com`
`agbizwichita[.]org`
`aphecalenterprises[.]com`
	Domain	In Horrid Hawk-Kampagnen verwendete gekaperte Domains

`thebagshelf[.]com`
`successbusinesspages[.]com`
`aventodesigns[.]com`
`twilliroll[.]com`
	Domain	In Hasty Hawk-Kampagnen verwendete gekaperte Domains

`aerospaceavenue[.]com`
`affixio[.]com`
`adventsales[.]co[.]uk`
`afarm[.]net`
`affiliatebash[.]com`
`amikamobile[.]com`
`afcmanager[.]net`
`adztrk[.]com`
`clickermediacorp[.]COM`
`mcpennsylvania[.]com`
	Domain	In Vacant Viper-Kampagnen verwendete gekaperte Domains

`mpinc[.]com`
`iccps[.]org`
`jmnet[.]com`
`ncbtv[.]com`
`uni-t[.]com`
`tmsec[.]com`
`mbhs[.]com`
	Domäne	In Vextrio Viper-Kampagnen verwendete gekaperte Domains

Indikator	Typ	Note
missouri[.]com mcpennsylvania[.]com	Domain	In Affiliate-Kampagnen von AntiBot Cloud verwendete gekaperte Domains
mosaicmedicalsupply[.]com	Domain	Von VexTrio GoRefresh verwendete gekaperte Domains
vipshopevent[.]su	Domain	In VexTrio GoRefresh Pharma-Kampagnen verwendete Domain
alonbyacarian[.]com fixedsights[.]com mygemcon[.]com sauda-pati[.]com tewksenterprises[.]com ummatie[.]com xiangmanlou[.]com	Domain	Von Gesundheitsbetrügern genutzte gekaperte Domänen
hXXps://ecole-artcom[.]com/wdown/ hXXps://www[.]mediasimulasi[.]com/wazxd	URL	Mit dem AsyncRAT-Download verknüpfte URLs
https://wercosliuhqgheirn[.]com/ hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php	URL	Mit dem DarkGate-Download verknüpfte URLs
hXXps://antibotcloudapi[.]com/9.php antibotcloudapi[.]com antibot[.]cloud antibotcloud[.]com ipv4[.]mikifox[.]com ipv6[.]mikifox[.]com admin[.]mikifox[.]com	FQDN	Im AntiBot Cloud-Dienst verwendete FQDNs

INFOBLOX THREAT INTEL

Infoblox Threat Intel ist der führende Anbieter von Original-DNS-Bedrohungsdaten und hebt sich von der Masse der Aggregatoren ab. Was zeichnet uns aus? Zwei Dinge: verrückte DNS-Kenntnisse und beispiellose Sichtbarkeit. DNS ist bekanntermaßen schwierig zu interpretieren und zu „jagen“, aber unser tiefes Verständnis und unser einzigartiger Zugang ermöglichen es uns, Cyberbedrohungen aufzuspüren. Wir sind proaktiv, nicht nur defensiv, und nutzen unsere Erkenntnisse, um Cyberkriminalität dort zu unterbinden, wo sie entsteht. Wir glauben auch an den Wissensaustausch, um die breitere Sicherheits-Community zu unterstützen, indem wir detaillierte Forschungsergebnisse und Indikatoren auf GitHub veröffentlichen. Darüber hinaus sind unsere Informationen nahtlos in unsere Infoblox DNS Detection and Response-Lösungen integriert, sodass Kunden automatisch von den Vorteilen profitieren und von extrem niedrigen Falsch-Positiv-Raten profitieren.

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com

Version: 20241030v1